IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) An apparatus for encrypting block data of a first size comprising:

encrypting sections connected in series, each of the encrypting sections comprising[[:]],

[[a]] first [[unit]] units each configured to randomize first subblock data which are obtained by dividing the block data[[;]], and

a second unit configured to diffuse data output from the first [[unit]] units with respect to the first size ~~a range which is wider than a range of the first subblock data~~ and supply a result of diffusion to [[a]] first [[unit]] units in a succeeding encrypting section, and wherein the first units and the second unit are configured to connect at least one input bit terminal of ~~bit of data input to~~ the first units ~~unit in own encrypting section being transmitted~~ to ~~at least~~ one ~~bit of data~~ input bit terminal of [[to]] the corresponding first unit in the succeeding encrypting section via at least two ~~routes~~ paths.

2 (Canceled).

3 (Canceled).

4. (Currently Amended) An apparatus for encrypting block data of a first size, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections comprising[[:]],

first nonlinear transformation units each configured to perform a nonlinear transformation process ~~over~~ for first subblock data which are obtained by dividing the block data[[;]], and

a first linear diffusion unit configured to perform a linear diffusion process for the first subblock ~~over~~ data output from the first nonlinear transformation units with respect to the first size ~~a range which is wider than a range of the first subblock data~~ and supply a result of the linear diffusion process to first nonlinear transformation units in a succeeding encrypting section,

wherein each of the first nonlinear transformation units comprises[[:]],

second nonlinear transformation units each configured to perform a nonlinear transformation process for ~~over~~ second subblock data which are obtained by dividing the first subblock data[[;]], and

a second linear diffusion unit configured to perform a linear diffusion process for the second subblock ~~over~~ data output from the second nonlinear transformation units with respect to the second size, ~~range of the first subblock data,~~ and

wherein the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal ~~bit of data input to one~~ of the first ~~second~~ nonlinear transformation units ~~in each of the encrypting sections is transmitted~~ to ~~at least~~ one ~~bit of data~~ input bit terminal of the corresponding first ~~to one of the second~~ nonlinear transformation units in the succeeding encrypting section via at least two ~~routes~~ paths.

5. (Currently Amended) The apparatus according to claim 4, wherein

input bit terminals of a second non-linear transformation unit are connected to input bit terminals of a corresponding second nonlinear transformation unit in the succeeding first

nonlinear transformation unit via at least two paths ~~the second nonlinear transformation unit in the first nonlinear transformation unit comprises a first half second nonlinear transformation units preceding the second linear diffusion unit and second half second nonlinear transformation units succeeding the second linear diffusion unit, and the first linear diffusion unit in each of the encrypting sections supplies an exclusive OR value of at least two outputs from the second half second nonlinear transformation units to at least one input to the first half second nonlinear transformation units in the succeeding encrypting section~~.

6. (Currently Amended) The apparatus according to claim 4, wherein

input bit terminals of more than one of the second nonlinear transformation units are connected to input bit terminals of corresponding second nonlinear transformation units in the succeeding first nonlinear transformation unit via at least two paths ~~the second nonlinear transformation unit in the first nonlinear transformation unit comprises a first half second nonlinear transformation units preceding the second linear diffusion unit and second half second nonlinear transformation units succeeding the second linear diffusion unit, and~~

~~the first linear diffusion unit in each of the encrypting sections supplies each exclusive OR value of at least two outputs from the second half second nonlinear transformation units to each input to the first half second nonlinear transformation units in the succeeding encrypting section~~.

7 (Canceled).

8. (Currently Amended) The apparatus according to claim [[7]] 4, wherein the block data is 128 bits in length, each of the first subblock data is 32 bits in length~~, and each of the second subblock data is 8 bits in length, the first linear diffusion unit performs a linear diffusion process on eight 16 bit data formed of corresponding bits each extracted from a~~

~~respective one of sixteen second subblock data while changing a bit extracted position~~.

9. (Original) The apparatus according to claim 4, wherein the first linear diffusion unit is implemented by hardware.

10. (Currently Amended) The apparatus according to claim 9, wherein an input-output characteristic of the first linear diffusion unit is based on multiplication in a ~~over the~~ Galois field.

11. (Original) The apparatus according to claim 5, wherein the first linear diffusion unit is implemented by software.

12. (Currently Amended) ~~An encryption apparatus based on a block encryption scheme comprising:~~

~~encrypting sections connected in series,~~

~~in which the first section receives 128-bit plaintext and each of the second section and later sections receives 128-bit block data processed by the preceding section, each of the encrypting sections comprising four first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of four sets of 32-bit data into which 128-bit block data is divided; and a first diffusion unit for performing a linear diffusion process using a maximum distance separable matrix on 128-bit block data in which four sets of 32-bit data output from the four first nonlinear transformation units are concatenated and outputting the processed 128-bit block data to the next stage;~~

~~four first nonlinear transformation units which are connected to first diffusion unit in the last encryption unit and receive 128-bit block data output from the first diffusion unit; and~~

~~a first key addition unit configured to receive four sets of 32-bit data output from the four first nonlinear transformation units and output 128-bit encrypted block data by adding~~

~~128-bit extended key data to 128-bit block data which is obtained by concatenating the four sets of 32-bit data output from those four first nonlinear transformation units,~~

~~wherein each of the first nonlinear transformation units comprises four second key addition units each of which adds 8-bit key data to a corresponding one of four sets of 8-bit data into which the 32-bit data is divided, four second nonlinear transformation units each of which performs nonlinear transformation on a corresponding one of the outputs of the second key addition units, a second diffusion unit for performing a linear diffusion process using a maximum distance separable table on 32-bit data obtained by concatenating the four sets of 8-bit data output from the four second nonlinear transformation units, and four sets of third key addition units and a third nonlinear transformation units connected to follow the second diffusion unit,~~

~~each of the first diffusion unit comprises a 16-bit diffusion unit for each of 8 bits for the second nonlinear transformation units in preceding and succeeding stages, the 16-bit diffusion unit performing a linear diffusion process through a 4 × 4 matrix operation based on multiplication over the Galois field $GF(2^4)$ or its equivalent circuit, the matrix operation being such that four bits at corresponding bits positions in four sets of 8-bit data from the four second nonlinear transformation units in one first nonlinear transformation section in the preceding stage are taken as one element on the input side of the matrix operation and four bits at corresponding bit positions in four sets of 8-bit data input to the four second nonlinear transformation section in one first nonlinear transformation processing section in the succeeding stage are taken as one element on the output side of the matrix operation, and~~

~~the 4 × 4 matrix operation based on multiplication over the Galois field $GF(2^4)$ in the 16-bit diffusion unit or its equivalent circuit transmitting, in any combination of one bit in the outputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the preceding stage and one bit in the inputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the succeeding stage, the state of that one bit in the preceding stage to that one bit in the succeeding stage over a plurality of operations paths.~~

An apparatus for encrypting block data of 128 bits, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections including,

four first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of 32 bits which are obtained by dividing the block data, and

a first linear diffusion unit configured to perform a linear diffusion process using a maximum distance separable matrix for the first subblock data output from the four first nonlinear transformation units with respect to the first size and supply a result of the linear diffusion process to four first nonlinear transformation units in a succeeding encrypting section;

a key addition unit which adds key data of 128 bits to output data of 128 bits from the encrypting section of the last stage,

wherein an encrypting section of a last stage comprises four nonlinear transformation units each configured to perform a nonlinear transformation process for the first subblock data of 32 bits,

wherein each of the first nonlinear transformation units includes stage sections, each stage section including,

four second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of 8 bits which are obtained by dividing the first subblock data,

a second linear diffusion unit configured to perform a linear diffusion process for the second subblock data output from the second nonlinear transformation units with respect to the second size, and

an adder for adding a key to four second subblock data of 8 bits input to the four second nonlinear transformation units,

wherein a stage section of a last stage comprises four second nonlinear transformation units each configured to perform a nonlinear transformation process for the second subblock data;

wherein the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encrypting section via at least two paths, and

wherein each of the four first nonlinear transformation units divides input data of 32 bits into eight groups of data of 4 bits which are formed of extracting the input data by every 8 bits, and the first linear diffusion unit comprises eight subunits each subunit receiving corresponding four groups of data of 4 bits output from the four first nonlinear transformation units, performing a 4×4 matrix operation based on multiplication over a Galois field $GF(2^4)$

for the received four groups of data of 4 bits, and outputting four groups of data of 4 bits to corresponding four first nonlinear transformation units (103) of the succeeding encrypting section.

13. (Currently Amended) ~~An encryption apparatus based on common key block encryption scheme comprising:~~

~~encrypting sections connected in series in which the first section receives 64-bit plaintext and each of the second section and later sections receives 64-bit block data processed by the preceding section, each of the encrypting sections comprising two first nonlinear transformation units each of which performs a local linear diffusion process and a nonlinear transformation process a corresponding one of two sets of 32-bit data into which 64-bit block data is divided; and a first diffusion unit for performing a linear diffusion process using a maximum distance separable matrix on 64-bit block data in which two sets of 32-bit data output from the two first nonlinear transformation units are concatenated and outputting the processed 64-bit block data to the next stage;~~

~~four first nonlinear transformation units which are connected to first diffusion unit in the last encryption unit and receive 64-bit block data output from the first diffusion unit; and~~

~~a first key addition unit configured to receive two sets of 32-bit data output from the two first nonlinear transformation units and output 64-bit encrypted block data by adding 64-bit common key data to 64-bit block data which is obtained by concatenating the two sets of 32-bit data output from those two first nonlinear transformation units,~~

~~wherein each of the first nonlinear transformation units comprises four second key addition units each of which adds 8-bit key data to a corresponding one of four sets of 8-bit data into which the 32-bit data is divided, four second nonlinear transformation units each of which performs nonlinear transformation on a corresponding one of the outputs of the second key addition units, a second diffusion unit for performing a linear diffusion process using a maximum distance separable table on 32-bit data obtained by concatenating the four sets of 8-bit data output from the four second nonlinear transformation units, and four sets of third key addition units and a third nonlinear transformation units connected to follow the second diffusion unit,~~

~~each of the first diffusion unit comprises a 16-bit diffusion unit for each of 8 bits for the second nonlinear transformation units in preceding and succeeding stages, the 16-bit diffusion unit performing a linear diffusion process through a 2×2 matrix operation based on~~

~~multiplication over the Galois field GF(2^4) or its equivalent circuit, the matrix operation being such that four bits at corresponding bits positions in four sets of 8-bit data from the four second nonlinear transformation units in one first nonlinear transformation section in the preceding stage are taken as one element on the input side of the matrix operation and four bits at corresponding bit positions in four sets of 8-bit data input to the four second nonlinear transformation section in one first nonlinear transformation processing section in the succeeding stage are taken as one element on the output side of the matrix operation, and~~

~~in the 2 × 2 matrix operation based on multiplication over the Galois field GF(2^4) in the 16-bit diffusion unit or its equivalent circuit transmitting, in any combination of one bit in the outputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the preceding stage and one bit in the inputs of a total 16 of second nonlinear transformation units in the four first nonlinear transformation processing units in the succeeding stage, the state of that one bit in the preceding stage to that one bit in the succeeding stage over a plurality of operations paths.~~

An apparatus for encrypting block data of 64 bits, the apparatus comprising:

encrypting sections connected in series, each of the encrypting sections including,

two first nonlinear transformation units each configured to perform a nonlinear transformation process for first subblock data of 32 bits which are obtained by dividing the block data, and

a first linear diffusion unit configured to perform a linear diffusion process using a maximum distance separable matrix for the first subblock data output from the four first nonlinear transformation units with respect to the first size and supply a result of the linear diffusion process to four first nonlinear transformation units in a succeeding encrypting section;

a key addition unit which adds key data of 128 bits to output data of 64 bits from the encrypting section of the last stage,

wherein an encrypting section of a last stage comprises two nonlinear transformation units each configured to perform a nonlinear transformation process for the first subblock data of 32 bits,

wherein each of the first nonlinear transformation units includes stage sections, each stage section including,

four second nonlinear transformation units each configured to perform a nonlinear transformation process for second subblock data of 8 bits which are obtained by dividing the first subblock data,

a second linear diffusion unit configured to perform a linear diffusion process for the second subblock data output from the second nonlinear transformation units with respect to the second size, and

an adder for adding a key to four second subblock data of 8 bits input to the four second nonlinear transformation units,

wherein a stage section of a last stage comprises four second nonlinear transformation units each configured to perform a nonlinear transformation process for the second subblock data,

wherein the first nonlinear transformation units, the first linear diffusion unit, the second nonlinear transformation units, and the second linear diffusion unit are configured to connect at least one input bit terminal of the first nonlinear transformation units to one input bit terminal of the corresponding first nonlinear transformation units in the succeeding encrypting section via at least two paths, and

wherein each of the two first nonlinear transformation units divides input data of 32 bits into eight groups of data of 4 bits which are formed of extracting the input data by every 8 bits, and the first linear diffusion unit includes eight subunits each subunit receiving corresponding two groups of data of 4 bits output from the two first nonlinear transformation units, performing a 2×2 matrix operation based on multiplication over a Galois field $GF(2^4)$ for the received two groups of data of 4 bits, and outputting two groups of data of 4 bits to corresponding two first nonlinear transformation units of the succeeding encrypting section.

14. (Currently Amended) A method for encrypting block data of a first size comprising:

randomizing first subblock data which are obtained by dividing the block data;

diffusing the randomized data with respect to the first size ~~a range which is wider than a range of the first subblock data~~; and

repeating the randomizing and the diffusing, wherein at least one bit input to the randomizing operation ~~two bits of the randomized data~~ is reflected on one bit input to the next randomizing operation via at least two paths ~~of data to be randomized next~~.

15. (Currently Amended) An article of manufacture comprising a computer readable medium ~~having~~ including a computer program embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize first subblock data which are obtained by dividing plaintext block data of a first size;

computer readable program code means for causing a computer to diffuse the randomized data with respect to the first size ~~a range which is wider than a range of the first subblock data~~; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least one bit input to the randomizing operation ~~two bits of the randomized data~~ is reflected on one bit input to the next randomizing operation via at least two randomizing and diffusing paths ~~of data to be randomized next~~.

16. (Currently Amended) An apparatus for decrypting encrypted block data comprising:

decrypting sections connected in series, each of the decrypting sections comprising[[:]],

[[a]] first [[unit]] units each configured to randomize first subblock data which are obtained by dividing encrypted block data[[;]], and

a second unit configured to diffuse data output from the first ~~unit~~ units with respect to the first size ~~a range which is wider than a range of the first subblock data~~ and supply a result

of diffusion to [[a]] first ~~unit~~ units in a succeeding encrypting section, and wherein the first units and the second unit are configured to connect at least one input bit terminal of ~~bit of data input to~~ the first units ~~unit in own encrypting section being transmitted~~ to ~~at least~~ one ~~bit of data~~ input bit terminal of [[to]] the corresponding first unit in the succeeding encrypting section via at least two ~~routes~~ paths.

17. (Currently Amended) A method for decrypting encrypted block data of a first size comprising:

randomizing first subblock data which are obtained by dividing the encrypted block data;

diffusing the randomized data with respect to the first size ~~a range which is wider than a range of the first subblock data~~; and

repeating the randomizing and the diffusing, wherein at least one bit input to the randomizing operation ~~two bits of the randomized data~~ is reflected on one bit input to the next randomizing operation via at least two paths ~~of data to be randomized next~~.

18. (Currently Amended) An article of manufacture comprising a computer readable medium ~~having~~ including a computer program embodied therein, the computer program comprising:

computer readable program code means for causing a computer to randomize first subblock data which are obtained by dividing encrypted block data of a first size;

computer readable program code means for causing a computer to diffuse the randomized data with respect to the first size ~~a range which is wider than a range of the first subblock data~~; and

computer readable program code means for causing a computer to repeat the randomizing and the diffusing, wherein at least one bit input to the randomizing operation ~~two bits of the randomized data~~ is reflected on one bit input to the next randomizing operation via at least two randomizing and diffusing paths ~~of data to be randomized next~~.